PURPOSE

This transmits Chapter 1, Basic Security Concepts, of new Handbook 1.16.8, Physical Security Standards, which replaces IRM 1(16)41, Physical and Document Security Handbook.

BACKGROUND

The IRM is being converted to a new format and style which willl be issued in 8½" x 11" instead of the current 6" x 9" size. The new IRM Handbook includes simplified text, a new numbering system, and a new format for organizing text.

The transmittal reissues existing information in the IRM format and provides new guidelines on facility, property and information protection. It replaces text currently contained in IRM 1(16)41 which is obsolete.

NATURE OF MATERIALS

New IRM Handbook 1.16.8, Physical Security Handbook, provides guidance and procedures for the protection of information, property and facilities.

Leland N. Keller
National Director, Real Estate
Planning and Management Division

Table of Contents

1.1 (02/26/99)
Overview

(1) The Internal Revenue Service has a legal obligation to protect the confidentiality of tax returns and related information. The Service also has responsibility for protecting the entire Federal Tax Administration System, not just the individual components of the system—employees, computer equipment, tax returns, monies, property, facilities and records.

(2) The Service has taken the position of providing reasonable protection commensurate with the character and value of the information or property involved. For example, service center operations require a high degree of physical protection to meet minimum security needs, while a small post-of-duty may require fewer protective measures.

(3) The Office of Management and Budget (OMB) has issued requirements for security of all Federal automated systems in OMB Circular A–130. OMB uses the term “Automated Information Systems Security Program” to refer to all security measures, including physical security safeguards. The Circular requires the head of each executive branch, department and agency to ensure that agency data (automated information) is adequately secured. This responsibility includes establishing physical, administrative and technical safeguards to protect personal, proprietary or other sensitive data whether it is national defense information or not.

1.2 (02/26/99)
Scope

(1) This handbook includes the physical security requirements for the entire Federal Tax Administration System as administered within the IRS. This includes all Service facilities (National Office, regions, host sites, districts, satellite offices, service centers, computing centers and other Service offices or space).

(2) This handbook establishes security guidelines for the reasonable protection of tax information, property, and facilities against disclosure, loss, damage, or destruction without unnecessarily restricting or interfering with operations. It also provides instructions on the Service’s Minimum Security Standards (MSS) and serves as a procedural and technical guide for security personnel. It includes optional methods for providing security under varying local conditions, provides for specific items requiring protection and identifies the various methods for protection.

1.3 (02/26/99)
Responsibilities

(1) The Chief, Management and Finance, has overall responsibility for the Servicewide physical security program. The National Director, Real Estate Planning and Management Division, is responsible for planning, developing, monitoring, evaluating and managing the Servicewide physical security program.

(2) Each Regional Commissioner is responsible for the implementation of an effective regional physical security program. Each District Director,

Service Center Director, Computing Center and Customer Service Center Director is responsible for implementing an effective physical security program and for ensuring that security measures taken are reasonable, adequate and effective. Regional Directors of Support Services are responsible for assuring that host sites are in compliance with Service policy and for providing guidance, oversight and assistance to the host site on the physical security program. Host Sites are responsible for implementing, evaluating and managing the physical security program and for providing guidance, oversight and assistance to client sites. The Director, Support Services Division (Headquarters Office), is responsible for planning, developing and evaluating the program for Headquarters facilities.

(3) National Office Division Directors are responsible for implementing an effective physical security program within their functional areas; for ensuring that security measures taken are reasonable, adequate and effective; and, for notifying the Real Estate Planning and Management Division of any proposed protective changes to items listed in Exhibit 1.16.8.5–2.

(4) To meet the obligation to provide necessary security protection to the Tax Administration System, the Service has determined that Service officials and managers are responsible for ensuring the continued operation of the Federal Tax Administration System by taking all responsible actions to prevent the loss of life and property, the disruption of services and functions and the unauthorized disclosure of documents and information.

(5) Managers are responsible for providing reasonable security for all information, documents, and property with which they are entrusted, for complying with all minimum security standards contained in 1.16.2, Managers Security Handbook, all local security requirements, and for reporting any violations to the respective Security function or other individuals who have security responsibilities. Managers must ensure that the physical security measures required for protecting information, property, and life are applied within their area of supervision and that those measures meet the established minimum security standards.

(6) All employees are responsible for providing reasonable security for all information, documents and property with which they are entrusted, for complying with established security procedures, all local security requirements, and for reporting any violations to their manager or to their respective Security functions or other individuals who have security responsibilities.

1.4 (02/26/99)

Basic Security Concepts

(1) Basic security concepts have been adopted by the Service and applied to the various activities within the Service. These concepts provide management with the flexibility to provide the degree of security or protection commensurate with the degree of sensitivity of each particular activity.

1.5 (02/26/99)
Evaluation of the Risk

(1) Evaluation of the risk is the first step in determining the degree of security required for a particular office. Security measures should be relative to the type of risks to which the facility and its contents are exposed, the probability that these risks will occur, and the impact that an occurrence would have on the organization. The Service recognizes the value of this approach and has developed a risk assessment process, contained in the Consolidated Physical Security Standards for IRS Facilities, for use throughout the Service.

(2) The next step is to review existing protective measures to determine their effectiveness. Security provided the facility as a whole and that provided by other tenants (if applicable) will affect the program developed for each office. Steps must be taken to maintain and evaluate protective measures implemented.

(3) The risk assessment process is to be used by the facility security personnel to develop a tailored physical protective system for the facility and associated annexes. The process provides an objective tool to identify and justify security requirements for IRS assets and systems that can be substantiated as minimum requirements to support IRS security policy. It allows the security analyst to independently assess the security situation at a specific facility, annex, or group of facilities and, based on this assessment, determine security criteria to protect the site(s).

1.6 (02/26/99)
Limiting Access

(1) The basic principle of security within IRS, or anywhere, is “limit access to assets based upon need.” When protecting information, for example, access to documents should be limited to those persons with a need to know the information. When the asset to be protected is a room, an area, a building a computer, or other such property, access to that property should be restricted to those persons who, due to their official duties and/or responsibilities, have a need for such access.

(2) Whether a person needs to access an asset will depend upon whether that access is necessary to enable the person to perform his/her assigned duties and responsibilities. Management is responsible for determining such a need and for subsequently deciding to grant or deny access. Once this determination has been made, management should consult Security personnel for assistance in selecting the appropriate method of achieving the desired control.

1.7 (02/26/99)
Safeguard Functions

(1) Most of the methods of protection are designed for protection after normal duty hours or at any time the assets to be protected are not under the personal custody of authorized Service employees.

(2) Because any single safeguard is often insufficient protection for any asset, the concept of layering of safeguards was developed to provide

security-in-depth. To facilitate understanding of security-in-depth, the following functions of safeguards are presented.

a. Deter — The psychological effect which a safeguard or a system of safeguards has upon the potential perpetrator or human originated threat is difficult to measure. One can determine the effectiveness of an alarm by the number of bonafide “catches” it makes, but we can only guess the effectiveness of a safeguard which is designed only or primarily to deter a human being. The best example of a pure deterrent is a sign which identifies a restricted area. While it would be ideal to have effective security simply by the use of such inexpensive means as signs, lights, and dummy TV cameras, it is not practical. A good security program will not rely solely upon safeguards which are only deterrents.
b. Delay — Ideally, the Service should be able to deny access to its assets to separate them from human originated threats. But this is not practical since to perform its mission the Service must allow access to its assets. The object then is to limit access to authorized personnel at approved times for official reasons. At times when the assets are not in the personal custody of an authorized IRS employee, they should be protected by means which delay as long as practical access by unauthorized persons. Safeguards such as locks, containers and walls will withstand (depending on the type of lock, container, etc.) forced entry and surreptitious entry attempts for a given period of time. This time is, hopefully, enough to discourage most would-be thieves, saboteurs, etc. However, given enough determination and resources (i.e., time, tools, and money) all such safeguards can be breached. If the asset being protected merits more than a deterring and delaying effort, the next function we would add is detection.
c. Detect — Many safeguards will automatically provide detection of an unauthorized act. For example, a door may show signs of a forced entry. However, an alarm might give evidence of an attempted surreptitious or forced entry. Depending once again upon the value of the asset, the timing of detection is crucial. For example, the goal for a threat such as sabotage of a computer in a service center would be to detect the attempted execution of the threat soon enough to intervene before it can be completed. Perimeter alarms and alarm activated cameras will help achieve this goal. Such a goal will also require a response force (internal IRS security personnel, contract guard personnel, Federal Protective Services, or the local police department) which will monitor detection devices and respond to them as appropriate. The functions of assessing, identifying, and tracking can be accomplished by closed circuit television (CCTV) systems, alarm systems and entry control systems. The most important of these functions is assessment, since the nature of the unauthorized act (e.g. unauthorized access, theft, robbery, assault, etc.) will influence the nature of the response to that act. Identifying a person committing an unauthorized act or a crime may be before, during or after the act has been committed. In some cases, we may only be able to respond to a threat as it is occurring. While the act

has not been prevented, identification of the perpetrator enables the Service to take appropriate action. The tracking function is most useful for the response force to focus on the current location of the problem or perpetrator.

d. Respond (Intervene/Apprehend) — Ideally response to a threat in progress is to detect it and to take appropriate action soon enough to prevent it from causing any harm or loss. To achieve this ideal, the delaying safeguard, the detection devices, and the response force must be designed to ensure that the safeguard delays the perpetrator long enough for a detection device to alert the response force and long enough to allow the response force to arrive in time to intervene to prevent access or to prevent a perpetrator from leaving the area with stolen government property or information. Realistically, we should expect a contract security force to respond to a threat at a service center within 5 minutes and at other buildings (protected with central station alarm systems) within 15 minutes. If this is not possible, then compensating measures must be included in the protective system design to delay an adversary until an effective response can be executed.

e. Deny — The only real way to accomplish this function is to destroy an asset to prevent unauthorized personnel from obtaining it. Clearly, for the Service, this only pertains to information on paper, microfilm, or magnetic media, etc. which is no longer needed or which is a waste by-product of a tax administration function.

(3) Exhibit 1.16. 8 1–1 shows the functions generally performed by certain physical security devices/techniques. No attempt is made to address the effectiveness of each, as this depends on the quality of the device selected. Also most of the techniques/devices shown are primarily for use against any potential perpetrator (employee or outsider) during unoccupied times. Conversely, ID media, electronic access control systems, sign in and other audit trail procedures and task separation techniques are generally for use during occupied times to protect against “insiders.”

1.8 (02/26/99)

Security Awareness

(1) A security program is enhanced when all managers and all employees are aware of security requirements including the reasons for each of the security requirements they are expected to follow or enforce. Each manager must know the general security requirements as well as the specific security measures which apply to his/her particular area of responsibility. The key to an awareness program is to show how the requirements relate to the work in which an employee is involved. For example, awareness efforts directed toward computer room employees should relate to security requirements in a computer room, while those efforts directed toward a tax auditor should relate to protecting the privacy of the taxpayer and the sensitivity to the tax return and return information.

(2) To ensure that all employees and managers are made aware of security requirements each security program will include an awareness program.

1.8.1 (02/26/99)
Methods of Dissemination

(1) There are numerous ways which security information can be disseminated to employees and managers. In addition to the security briefing (see below), the following methods will be considered as tools of the security awareness program:

a. In-house newsletters — may be used to present articles that will appeal to the target audience and will maintain a continuing interest;
b. Memoranda — may be used to stress a particular requirement which may be new or not being followed;
c. Stuffers — graphic presentation that can be disseminated with other all employee items (i.e. earning statements);
d. Posters — graphic presentations that may be posted in heavy traffic areas or in areas where a particular requirement applies;
e. Flyers — may be used to make a particular point or to stress a new requirement or one which is not being followed;
f. Managers meetings — may be used to discuss security items of common interest to the managers;
g. Employee meetings — may be used by managers to present current issues to employees or for discussion.

1.8.2 (02/26/99)
Security Briefings

(1) The security awareness program will as a minimum include briefings as specified below:

a. The Director and Assistant Director at each service center, computing center and district will be given a security briefing by Host Site security personnel, shortly after being appointed. The briefing will include current information on threats to the Service, and a review of the director's responsibilities in maintaining properly protected facilities.
b. National office executives at the division director level and above will be given a security briefing by the Headquarters Operations security staff. The briefing will include current information on threats to the Service and a review of the official's responsibilities.
c. All managerial personnel will be given annual security briefings on their responsibilities by security personnel. The information presented during these sessions must then be passed on by the managers to all their employees. Security items will also be made a regular topic at periodic group/staff meetings.
d. All new employees will receive a security orientation within the first week following employment. The orientation will be given separately or as part of the existing new employee orientation.
e. All WAE's will be given a refresher security orientation within the first week if they have been in a non-work status for nine months or longer. Local management will determine who will provide the orientation.
f. Periodic security briefing sessions will be conducted for all service center supervisors throughout the year and at the beginning of each filing season. Corporation Education Branch at each facility will schedule all the first-line managers to attend the security briefing session before the start of each filing period. The individual sessions

should be conducted by each facility's security personnel and Disclosure Officer with introductory remarks by the director or assistant director (if scheduling permits). Special scheduling considerations will be necessary to accommodate managers who work on shifts or off-site locations.

g. Management will inform each employee of special security requirements pertaining to their particular work area or facility within the first 30 days the employee reports to the manager for duty.

This page intentionally left blank.

Exhibit 1.16.8.1-1 (02/26/99)
Safeguards and Their Related Protection Functions

Note: The functions of each safeguard may vary according to the quality of the safeguard and the nature of the threat. The following chart represents generally the functions each safeguard provides. Not included here are other functions such as promoting awareness of security to meet responsibilities to prevent violations or crimes, and investigation and appropriate remedial actions for violations. These are not within the scope of the manual.

Safeguards	Deter	Delay	Detect	Assess	Identify	Track	Respond		Deny Access
							Inter-vene	Appre-hend	
Alarms	x		x	x*	x	x	x**	x**	
Areas	x	x	x		x				
Buildings	x	x	x						
CCTV	x		x	x	x	x			
Containers	x	x	x						
Degaussers Document Destructors and Shred-ders									x
Entry Control Systems	x		x	x	x	x			
Fences	x	x							
Guards	x	x	x	x	x	x	x	x	
ID Media Systems	x		x		x				
Locks	x	x	x						
Procedures (e.g. Audit Trail)	x		x		x	x			
Secured Ar-eas Security Rooms	x	x	x						
Signs	x								

Exhibit 1.16.8.1-1 (Cont. 1) (02/26/99)
Safeguards and Their Related Protection Functions

Task Separation Compartmentation	x							

*Alarms can be arranged to determine the extent of a fire (by zoning) or the nature of unauthorized entry (by duress to an authorized entrant).

** Alarm systems can be designed to provide for a response force; by themselves of course, they merely annunciate an unauthorized access. Programmed into an integrated system can be instructions to automatically shut doors, operate cameras, start/stop sprinklers, or perform other actions which go beyond detection and assessment of a threat to intervening or, as in the case of some entry controls, rejecting personnel who attempt an unauthorized access.